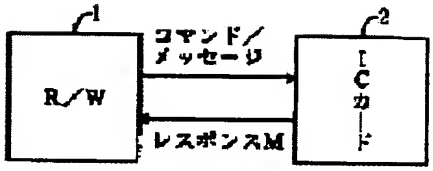
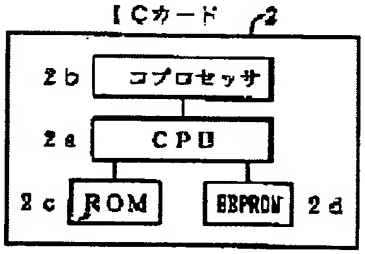
IC CARD HAVING PROVISION AGAINST ATTACK TAKING ADVANTAGE OF FAILURE

Patent number: JP11008616
Publication date: 1999-01-12
Inventor: HANDA FUKIO
Applicant: DAINIPPON PRINTING CO LTD
Classification:
- international: H04L9/10; G06K19/073; G09C1/00; G09C1/00; H04L9/32
- european:
Application number: JP19970159992 19970617
Priority number(s):

Abstract of **JP11008616**

PROBLEM TO BE SOLVED: To enhance the security against attach taking advantage of a failure of the IC card that conducts signature generating processing at a high speed by using the Chinese remainder theorem. SOLUTION: The power remainder calculation generating a digital signature M is processed at a high speed with the Chinese remainder theorem by using a prime factor to modulus (n), and an error check code for data generated in the calculation process of the Chinese remainder theorem together with the data themselves are calculated and stored simultaneously. In the case of the digital signature M, the error check code of the data is again calculated, the stored error check code is collated to detect an error of the data and an error status is returned when the error is detected.





Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－8616

(43)公開日　平成11年(1999)１月12日

(51)Int.Cl.[6]	識別記号	FI	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ｚ
Ｇ０６Ｋ　19/073		Ｇ０９Ｃ　1/00	６５０Ｚ
Ｇ０９Ｃ　1/00	６５０		６６０Ｚ
	６６０		６６０Ａ
		Ｇ０６Ｋ　19/00	Ｐ

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平9－159992

(22)出願日　平成９年(1997)６月17日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　半田富己男
東京都新宿区市谷加賀町一丁目１番１号大日本印刷株式会社内

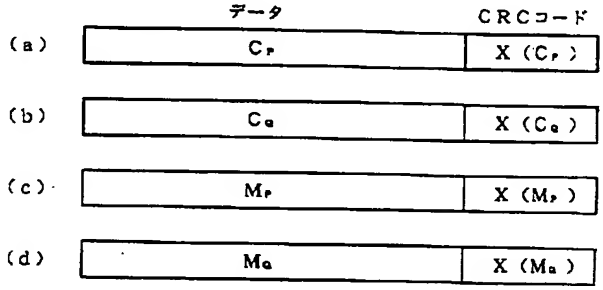
(74)代理人　弁理士　鍾川　昌信　（外７名）

(54)【発明の名称】　故障利用攻撃対応ＩＣカード

(57)【要約】

【課題】　中国人剰余定理を利用して高速に署名作成処理をするＩＣカードの故障利用攻撃に対する安全性を高める。

【解決手段】　ディジタル署名の作成を行う冪乗剰余計算を法ｎの素因数を用いて中国人剰余定理により高速で処理し、中国人剰余定理による計算過程において生成されるデータとともに、該データについてのエラー検出符号を同時に計算して記憶しておき、ディジタル署名の作成の際に、前記データのエラー検出符号を再度計算し、記憶しておいたエラー検出符号と照合してデータの誤りを検出し、誤りを検出した時にはエラーステータスを返すようにしたことを特徴とする。



ステップ2：$M_p=C_p^x \bmod p$　、$M_q=C_q^y \bmod q$　……（６）

ここに、$x=d_p$、$y=d_q$を計算する。ステップ2での計算は、ｐ、ｑ各々についての通常のＲＳＡ復号化計算である。この結果を用いると、（１）式は次の連立合同式に帰着する。

$M \equiv M_p \pmod p$　……（７）

$M \equiv M_q \pmod q$　……（８）

（７）式は$M-M_p$がｐで割り切れ、（８）式は$M-M_q$がｑで割り切れることを表している。

ステップ3：中国人剰余定理より、

$M=\{a(M_p-M_q) \bmod p\} \times q + M_q$　……（９）

の計算でディジタル署名Ｍが求められる。

【００09】図7は上記した手順で高速でディジタル署名Ｍを作成する処理フローを示している。ＩＣカード２がディジタル署名のコマンドを受け取ると（実際にはコマンド名を受け取り、コマンド名に対応するコマンドをＲＯＭから読みだす）、ＩＣカードではあらかじめＥＥＰＲＯＭに記憶してあるd_p、d_q、ａを読み出すとともに、コマンドとともに送られてくるメッセージを読み込む（ステップ１～２）。次いで、（５）式により$C \bmod p$、$C \bmod q$を計算してC_p、C_qを求め（ステップ３～４）、次いで、C_p、C_q、d_p、d_q、ｐ、ｑを用い、（６）式でM_p、M_qを計算する（ステップ５～６）。次いで、中国人剰余定理により（９）式を用いてディジタル署名Ｍを作成し、作成したディジタル署名Ｍをレスポンスとしてリーダ／ライタ１へ返す。

【００10】このように、ｎに対して半分の桁数のｐ、ｑによる剰余計算となるため、（１）式の計算に比して計算量がほぼ1／4となり、処理を高速化できる。

【００11】ところで故障利用攻撃では、ディジタル署名を作成するＩＣカードに対して、外部から物理的刺激（熱、圧力、放射線、電圧等）を加えることにより、ＩＣカードのメモリやレジスタ上のビットパターンの一部に故意に誤りを発生させる。例えば、前記ステップ2の（６）式の計算途中で、故意に誤りを発生させ、M_pまたはM_qのどちらか一方の値を誤らせる。ここでは、M_pの計算結果が誤っているとしてそれをM_p'とし、M_qは正しく求められているとする。M_p'、M_qを（９）式に適用して求めた署名Ｍも誤っていることになるから、それをＭ′とする。

【００12】このとき、署名対象データＣと公開されている法ｎの値を使って、

$gcd((M')^e-C, n)$（ｇｃｄ：最大公約数）　……（１０）

によって秘密に保つべきｎの素因数ｑが求められてしまう（Marc Joye and Jean-Jacques Quisquater,"Attacks on system using Chinese remaindering" November 1,1996この論文はhttp://www.dice.ucl.ac.be/crypto/techreports.htmlにて公開されている）。なぜならば、Ｍが正しいとすると

$M^e \equiv C \pmod n$　……（１１）

が成立するが、M_p'に誤りがあるため成立しない。そして

$M_p' \equiv C_p^x \pmod p$　$(x=d_p)$　……（１２）

なので、

$(M')^e \equiv C \pmod q$

である。すなわち、$(M')^e-C$とｎ（$=pq$）との最大公約数はｑである。こうして、ｑが分かるとｐも分かり、その結果、すべての秘密情報が分かってしまうことになる。

【００13】

【発明が解決しようとする課題】このように、故障攻撃により秘密情報が解析されるため、中国人剰余定理を利用して計算したディジタル署名Ｍが正しいか否かを確認する必要があるが、確認するには、作成されたディジタル署名を署名作成者自ら検証してみる必要があった。すなわち、署名作成者の公開鍵ｅを用いて$M^e \equiv C \pmod n$を検証する必要があった。

【００14】ところで、冪乗剰余計算を高速に処理するコプロセッサを搭載したＩＣカードの場合、コプロセッサによる冪乗剰余計算の対象となる整数の大きさはハードウェア的に制限がある。前述したように、高速処理のためにディジタル署名の作成において冪乗剰余計算の法ｎの素因数ｐ、ｑを用いるので、ｐ、ｑの大きさをコプロセッサで扱える限度いっぱいまでとると、ｐ、ｑの積であるｎはコプロセッサで扱える限度を超えてしまう。署名の検証はｅ，ｎのみ用いて$M^e \equiv C \pmod n$をコプロセッサで演算して行うが、この演算を行うことができなくなってしまう。一方、ＣＰＵの命令を用いてソフトウエアでの処理により検証すると、署名の作成本体処理よりもはるかに多くの時間を要するため、故障利用攻撃を受けたかどうかの検証を実用的なレスポンス時間内に行うことができない。そのため、ｎの大きさがコプロセッサで扱える限度を超える場合には、作成した署名の検証を行わないことが一般的であり、故障利用攻撃を許してしまう結果となっていた。

【００15】本発明は上記課題を解決するためのもので、メッセージ作成者本人がＲＳＡ秘密鍵を用いてディジタル署名を作成する際に、中国人剰余定理を利用して高速に署名作成処理をするＩＣカードに対して、中国人剰余定理の途中結果に計算誤りを発生させ、誤ったディジタル署名を作らせることによって、秘密情報を得よう

ジタル署名作成処理フローを説明する。ＩＣカードがディジタル署名のコマンドを受け取ると、ＩＣカードではあらかじめＥＥＰＲＯＭに記憶してあるｄｐ、ｄｑ、ａを読み出すとともに、コマンドとともに送られてくるメッセージを読み込む（ステップ１１～１２）。次いで、（５）式によりＣ mod p を計算してＣｐを求めるとともに、ＣｐのＣＲＣコードＸ（Ｃｐ）を計算して記憶する（ステップ１３）。同様に、Ｃ mod q を計算してＣｑを求めるとともに、ＣｑのＣＲＣコードＸ（Ｃｑ）を計算して記憶する（ステップ１４）。また、（６）式でＭｐ、Ｍｑを計算するとともに、Ｍｐ、ＭｑのＣＲＣコードＸ（Ｍｐ）、Ｘ（Ｍｑ）を計算してそれぞれ記憶する（ステップ15、１６）。次いで、ディジタル署名を作成する段階で、再びＣｐ、Ｃｑ、Ｍｐ、ＭｑのＣＲＣコードを計算し、記憶しておいたＣＲＣコードＸ（Ｃｐ）、Ｘ（Ｃｑ）、Ｘ（Ｍｐ）、Ｘ（Ｍｑ）とそれぞれ照合する（ステップ１７～２０）。

【００２４】この照合は、図4 に示すように、記憶しておいたＣＲＣコードＸ（Ｙ）と、計算したＹのＣＲＣコードＴとを比較し、両者が一致すれば正常終了、一致しなければ異常終了とする。図3 のステップ１７～２０のどの段階で異常終了となっても、その時点でエラーのステータスワードをリーダ／ライタに返して処理を終了する。ステップ１７～２０がすべて正常終了の場合、ディジタル署名を作成して、これをレスポンスとして返す（ステップ２１、２２）。

【００２５】【発明の効果】以上のように本発明によれば、ｎの大きさがコプロセッサで扱える限度を超える場合にも、作成した署名の検証を短時間で行うことができるので、故障利用攻撃を受けても、誤ったディジタル署名をレスポンスとして返してしまう可能性を減らすことができる。故障利用攻撃によって、エラー検出符号そのものに誤りが発生したり、エラー検出符号の誤り検出能力を超える範囲の誤りが発生する可能性が全くないとはいえないが、ほとんどの場合において故障利用攻撃を受けたことを検出することが可能である。

【図面の簡単な説明】

【図1】エラー検出符号としてＣＲＣコードを用いた例を説明する図である。

【図2】エラー検出符号としてパリティチェックを用いた例を説明する図である。

【図3】本発明のディジタル署名作成処理フローを説明する図である。

【図4】ＣＲＣ照合処理を説明する図である。

【図5】リーダ／ライタとＩＣカードとの通信を説明する図である。

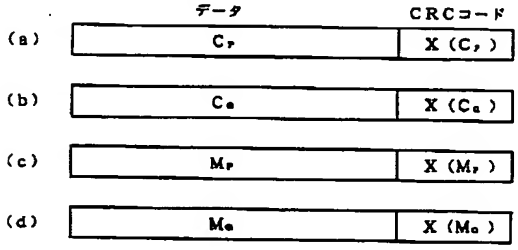
【図6】ＩＣカードの説明図である。

【図7】従来のディジタル署名作成処理フローの説明図である。

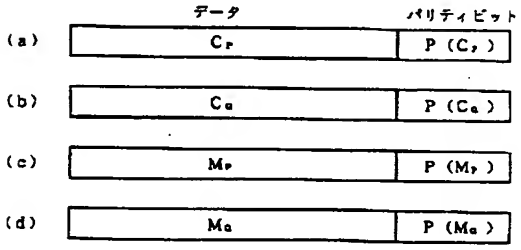
【符号の説明】

1…リーダ／ライタ、２…ＩＣカード、２ａ…ＣＰＵ、２ｂ…コプロセッサ、２ｃ…ロム、２ｄ…ＥＥＰＲＯＭ。

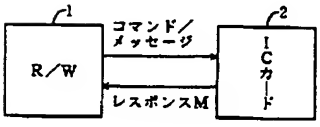
【図1】



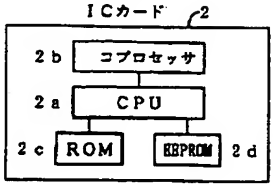
【図2】



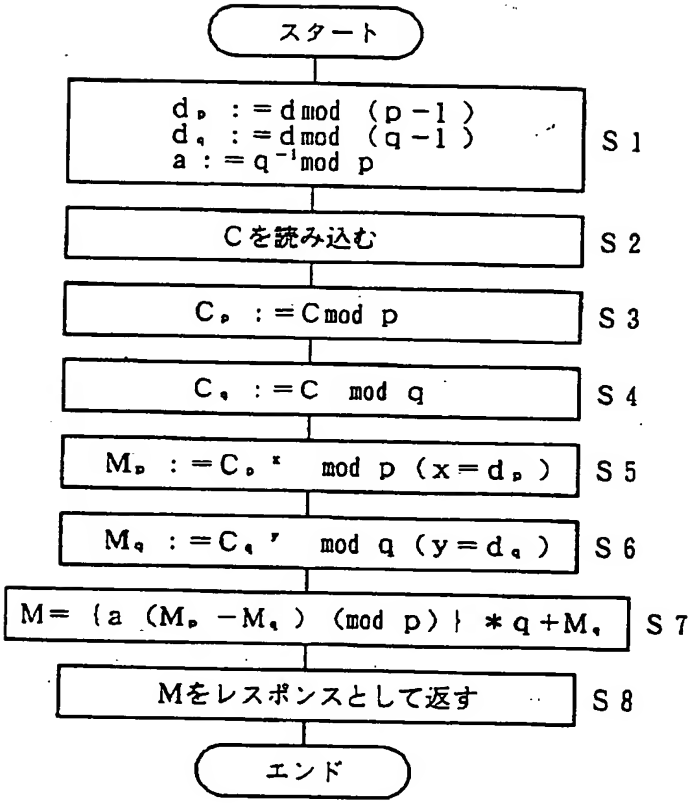
【図5】



【図6】



【図7】



フロントページの続き

(51)Int.Cl.[6]　識別記号　　FI
H04L 9/32　　H04L 9/00　673E